

# Security Target DTCO 1381, Release 1.3v Digital Tachograph - Vehicle Unit

**Author:** Winfried Rogenz, I CV AM TTS LRH


Siemens VDO Automotive AG  
Heinrich-Hertz-Straße 45  
D-78052 Villingen-Schwenningen  
Postfach1640  
D-78006 Villingen-Schwenningen  
Tel: +49 7721 / 67 - 2147  
Fax: +49 7721 / 67 – 79 2147  
E-Mail: [winfried.rogenz@continental-corporation.com](mailto:winfried.rogenz@continental-corporation.com)

**Revision:** 1.15.1.0

**Status:** Final

**File:** Security Target\_V.doc

**Release** DTCO 1381 Release 1.3v

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
			Document	Version	Pages
			40225345 SPE 000 AB		1 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## 1 History of changes

Version	Date	Author, editor	reason
1.0	30.03.2000	Rogenz, Winfried, LM/ZU	rough draft
2.0	11.10.2000	Rogenz, Winfried, LM/ZU	draft
3.0	24.11.2000	Rogenz, Winfried, LM/ZU Lindinger, Andreas, LE/FF Näther Horst, LE/FF	revision together with LE/FF
4.0	01.12.2000	Rogenz, Winfried LM/ZU	completion for evaluation
4.1	23.03.2001	Rogenz, Winfried LM/ZU	revision after evaluation Final release
4.2	09.10.2002	Rogenz, Winfried LBDZU	revision after publication of Annex I(B) (CR (EC) No. 1360/2002 Final release
4.3	03.06.2004	Rogenz, Winfried	Revision after publication of amendment of 3821/85 by CR (EC) No. 432/2004
0403.01 Rev. 1.6)	10.06.2005	Rogenz, Winfried TCO H	Adaptation for Release 1.2
0403.01 Rev. 1.7)	07.07.2005	Rogenz, Winfried TCO H	Revision after evaluation Final release
0403.01 Rev. 1.8)	08.07.2005	Rogenz, Winfried TCO H	Revision after evaluation Final release
0403.01 Rev. 1.9)	02.08.2005	Rogenz, Winfried TCO H	Revision for certification Final release
0403.01 (Rev. 1.10)	03.05.2006	Winfried Rogenz TCO H	2. Revision for certification Final release
Rev. 1.11	08.06.2006	Zalan Szilagyi	Accept all changes for Release_1.2_DocFinish
1.11.1.0	2007-02-16	Adrian Farcas	Update for Release 1.2a
1.11.1.1		Rogenz	No changes
1.11.1.2	2007-03-01	Müller F.	New PDM Number
1.11.1.3	2007-03-02	Rogenz, Winfried, SV CV Div TCO H	completion for evaluation
1.11.1.4	2007-03-02	Rogenz, Winfried, SV CV Div TCO H	Editorial corrections
1.11.1.5	2007-06-13	Friedrich Müller	Accept all changes for Rel1.2a
1.13	2007-06-13	Friedrich Müller	Prepare document for Rel1.3
1.14	2007-10-25	Rogenz Winfried	Update for Release 1.3
1.15	2007-11-14	Rogenz Winfried	Correction after review
1.15.1.0	2012-04-25	Rogenz Winfried	Update for Release 1.3v

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB			Version	Pages 2 / 52	



# SECURITY TARGET DTCO 1381, Release 1.3v

## 2 List of contents

<b>1</b>	<b>History of changes .....</b>	<b>2</b>
<b>2</b>	<b>List of contents.....</b>	<b>3</b>
<b>3</b>	<b>Introduction .....</b>	<b>4</b>
<b>4</b>	<b>Abbreviations and definitions .....</b>	<b>5</b>
4.1	Abbreviations .....	5
4.2	Definitions .....	5
<b>5</b>	<b>Product rationale .....</b>	<b>7</b>
5.1	Vehicle Unit description and method of use .....	7
5.2	Vehicle Unit life cycle .....	14
5.3	Subjects, objects, and access rights .....	16
5.4	Threats .....	21
5.5	Security objectives .....	22
5.6	Information Technology Security Objectives .....	22
5.7	Physical, personnel or procedural means .....	23
<b>6</b>	<b>Security enforcing functions .....</b>	<b>25</b>
6.1	Identification and authentication .....	26
6.2	Access control .....	29
6.3	Accountability .....	33
6.4	Audit .....	37
6.5	Object reuse .....	39
6.6	Accuracy .....	40
6.7	Reliability of service .....	42
6.8	Data exchange .....	44
6.9	Cryptographic support.....	45
<b>7</b>	<b>Definition of security mechanisms .....</b>	<b>46</b>
<b>8</b>	<b>Minimum strength of security mechanisms .....</b>	<b>46</b>
<b>9</b>	<b>Level of assurance .....</b>	<b>46</b>
<b>10</b>	<b>Rationale .....</b>	<b>47</b>
<b>11</b>	<b>References .....</b>	<b>52</b>

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					3 / 52

3 Introduction


This document contains a description of the vehicle unit DTCO 1381, Release 1.3v ( the TOE), of the threats it must be able to counteract and of the security objectives it must achieve. It specifies the required security enforcing functions. It states the claimed minimum strength of security mechanisms and the required level of assurance for the development and the evaluation.

This document is based on the Vehicle Unit Generic Security Target, which is described in Appendix 10 <sup>1</sup> of Annex 1B <sup>2</sup> of the European Regulation (EEC) No 3821/85 <sup>3</sup> amended by the European Regulation (EEC) No 2135/98 <sup>4</sup> and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006 .The document states the security functions and assumptions on the environment and describes how they are implemented in the vehicle unit DTCO 1381. . Wherever it is referred to DTCO 1381, it deals with the current TOE DTCO 1381, Release 1.3.v

Requirements referred to in the document, are those of the body of Annex 1B. For clarity of reading, duplication sometimes arises between Annex 1B body requirements and security target requirements. In case of ambiguity between a security target requirement and the Annex 1B body requirement referred by this security target requirement, the Annex 1B body requirement shall prevail.

Annex 1B body requirements not referred by security targets are not the subject of security enforcing functions.

Unique labels have been assigned to threats, objectives, procedural means and SEF specifications for the purpose of traceability to development and evaluation documentation.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
	Designation				
	Security Target DTCO 1381, Release 1.3				
Document			Version		
40225345 SPE 000 AA			Pages		
			4 / 52		


## 4 Abbreviations and definitions

### 4.1 Abbreviations

<b>CAN</b>	Controller Area Network
<b>DTCO</b>	Digital Tachograph
<b>EQT<sub>i</sub>.C</b>	equipment certificate
<b>EQT<sub>i</sub>.SK</b>	equipment private key
<b>EQT<sub>i</sub>.PK</b>	equipment public key
<b>EUR.PK</b>	European public key
<b>K<sub>m</sub></b>	Master key
<b>K<sub>m<sub>VU</sub></sub></b>	Part of the Master key, will manage the pairing between a motion sensor and the vehicle unit
<b>K<sub>id</sub></b>	Individual device key for protection of the session key between motion sensor and vehicle unit
<b>K<sub>sm</sub></b>	Session key between motion sensor and vehicle unit
<b>K<sub>st</sub></b>	Session key between tachograph cards and vehicle unit
<b>MS<sub>i</sub>.C</b>	Member State certificate
<b>PIN</b>	Personal Identification Number
<b>ROM</b>	Read Only Memory
<b>SEF</b>	Security Enforcing Function
<b>TBD</b>	To Be Defined
<b>TOE</b>	Target Of Evaluation
<b>VU</b>	Vehicle Unit

### 4.2 Definitions

<b>Digital Tachograph</b>	Recording Equipment.
<b>Entity</b>	A device connected to the VU (specific definition see S1).
<b>Management Device</b>	A dedicated device for software upgrade of the TOE
<b>Motion data</b>	The data exchanged with the VU, representative of speed and

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation Security Target DTCO 1381, Release 1.3					
 Document 40225345 SPE 000 AA				Version	Pages
					5 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

## Motion Sensor

distance travelled (specific definition see O17).

## Physically separated parts

Part of the recording equipment, providing a signal representative of vehicle speed and/or distance travelled.

## Security data

Physical components of the vehicle unit that are distributed in the vehicle as opposed to physical components gathered into the vehicle unit casing.

## SW-Upgrade

The specific data needed to support security enforcing functions (e.g. crypto keys) (specific definition see O2, O3).

## SW-Upgrade Modul (SWUM)

SW-Upgrade installs a new version of software in the TOE.

## System

A component of software in the TOE which is responsible for the realization and control of the software upgrade

## Tachograph cards

Equipment, people or organisations, involved in any way with the recording equipment.

Smart cards intended for use with the recording equipment. Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. A tachograph card may be of the following types:

- driver card,
- control card,
- workshop card,
- company card.

## User

Users are to be understood as human user of the equipment. Normal users of the VU comprise drivers, controllers, workshops and companies (specific definition see S2).


## User data

Any data, other than security data, recorded or stored by the VU, required by Chapter III.12. (specific definition see O1, O4 to O16).

## Vehicle Unit

The recording equipment excluding the motion sensor and the cables connecting the motion sensor. The vehicle unit may either be a single unit or be several units distributed in the vehicle, as long as it complies with the security requirements of this regulation.

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
	Designation				
	Security Target DTCO 1381, Release 1.3				
Document			Version		Pages
40225345 SPE 000 AA					6 / 52

Ot: Observe  
Pri: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

5 Product rationale

5.1 Vehicle Unit description and method of use

The VU is intended to be installed in road transport vehicles. Its purpose is to record, store, display, print and output data related to driver activities. It is connected to a motion sensor with which it exchanges vehicle's motion data.

Users identify themselves to the VU using tachograph cards.

The VU records and stores user activities data in its data memory, it also records user activities data in tachograph cards. The VU outputs data to display, printer and external devices.

The vehicle unit's operational environment while installed in a vehicle is described in the following figure:

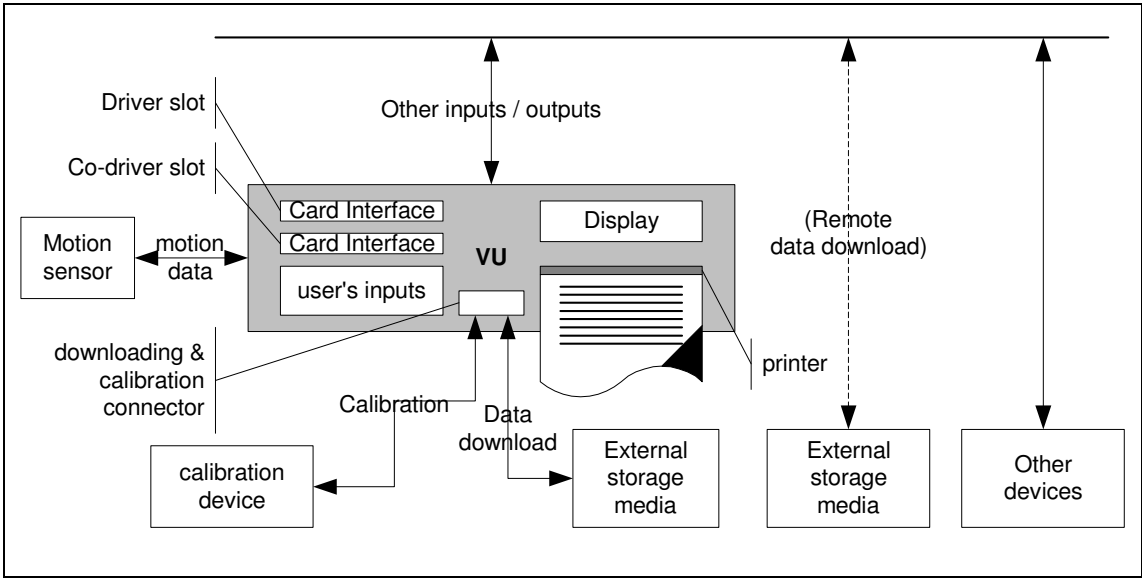


Figure 1 VU operational environment

The VU general characteristics, functions and mode of operations are described in Chapter II of Annex 1B. The VU functional requirements are specified in Chapter III of Annex IB.

The typical VU is described in the following figure. It must be noted that although the printer mechanism is part of the TOE, the paper document once produced is not.

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					7 / 52



Qt: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

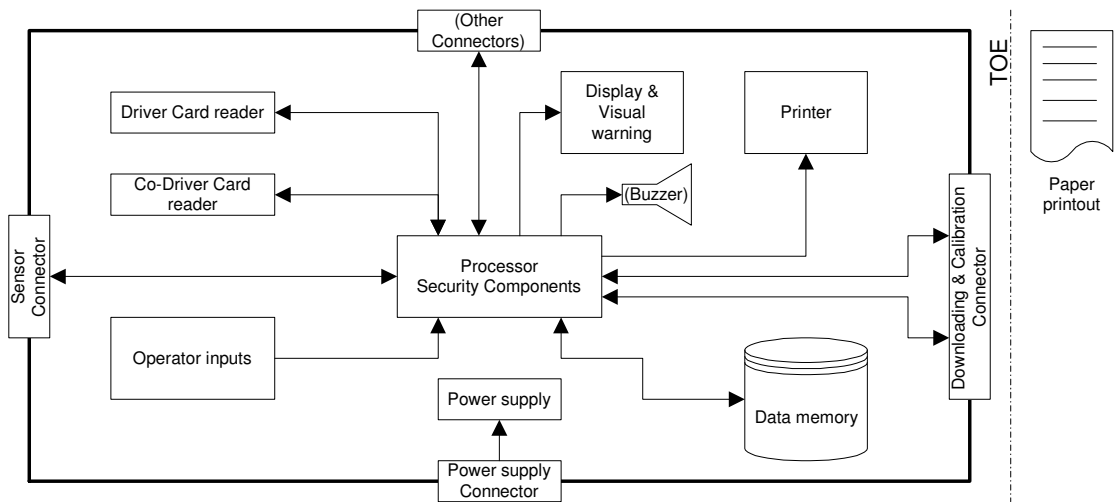


Figure 2 Typical VU (...) optional

5.1.1 Implementation in the TOE

The DTCO 1381 fulfils the description and method of use as described in section 5.1. The following figure shows the basic architecture of the actual TOE, the DTCO 1381:

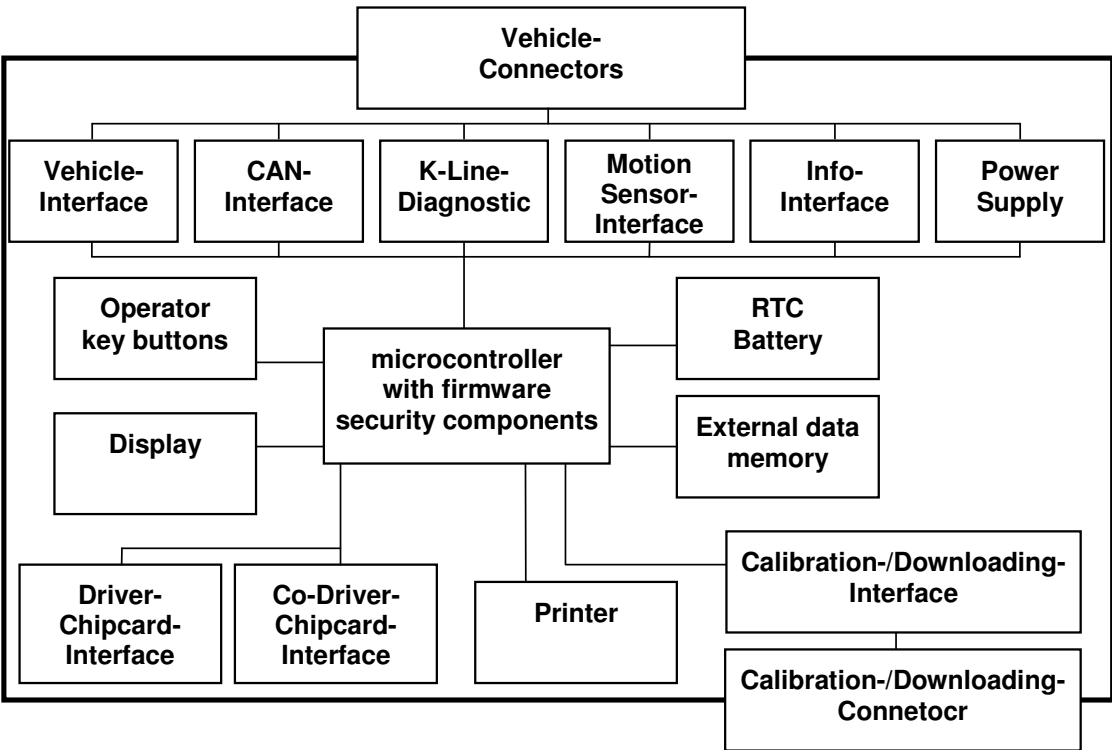



Figure 3 Basic architecture TOE DTCO 1381

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by		Date	Department	Released by	Date	Department
				Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
		Designation Security Target DTCO 1381, Release 1.3				
		Document 40225345 SPE 000 AA				Version 8 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

The Scope of supply of the TOE includes the DTCO 1381 and the appropriate manuals.

The following description shows the general functions implemented in the TOE.

## 5.1.2 General functions in the TOE:

### (1) *monitoring tachograph cards insertions and withdrawals*

The TOE monitors two chip card interfaces ( for a driver and a co-driver) to detect tachograph card insertions and withdrawals.

Upon tachograph card insertion the TOE detects:

- whether the card inserted is a valid tachograph card;
- and in such a case identifies the card type.

### (2) *speed and distance measurement*

Vehicle speed and distance are recorded using the real-time signal of the motion sensor.

The current speed value is stored every second in the data memory over a driving time of 24 hours. The speed resolution value is 1 km/h, the speed range is 0 km/h up to 220 km/h.

The distance resolution value is 0,1 km, the distance range is 0 km up to 9 999 999,9 km.

The TOE records speed profiles as an optional feature.

### (3) *time measurement*

The TOE incorporates a real-time clock buffered by a battery. The basis for the measurement is the required UTC-format. The time resolution value is 1 sec.

### (4) *monitoring driver activities*

The TOE permanently and separately monitors the activities of one driver and one co-driver as DRIVING, WORK, AVAILABILITY, or BREAK/REST.

With the operator key buttons the driver and/or the co-driver can manually select WORK, AVAILABILITY, or BREAK/REST.

When the vehicle is moving, the TOE selects automatically DRIVING for the driver and AVAILABILITY for the co-driver.

### (5) *monitoring driving status*

The TOE selects the driving status CREW when two valid driver cards are inserted in the equipment, the driving status SINGLE is selected in any other case.

### (6) *drivers manual entries*

With the operator key buttons on the front panel of the TOE the driver and/or the co-driver have the possibility to manually enter the places where the daily work periods begin and/or end.

After card insertion the cardholder can manually enter activities, with their dates and times of beginning and end, among WORK or AVAILABILITY or BREAK/REST only, strictly included within the period last card withdrawal – current insertion only.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					9 / 52



# SECURITY TARGET DTCO 1381, Release 1.3v

The driver can enter, in real time, the following two specific conditions: "OUT OF SCOPE" (begin, end) and "FERRY / TRAIN CROSSING".

## (7) company locks management

This function of the TOE manages the locks placed by a company to restrict data access in company mode to itself. Locking-in is possible at the insertion of a company card.

Locking-out is only possible for the company whose lock is "in" or if another company locks in. A previous locked-in company will then be automatically locked-out.

## (8) monitoring control activities

This function of the TOE monitors DISPLAYING, PRINTING, VU and card DOWNLOADING activities carried out while in control mode. This function also monitors OVER SPEEDING CONTROL activities while in control mode.

## (9) detection of events and/or faults

The following events and faults are detected and stored:

- "Insertion of a non valid card" event
- "Card conflict" event
- "Time overlap" event
- "Driving without an appropriate card" event
- "Card insertion while driving" event
- "Last card session not correctly closed" event
- "Over speeding" event
- "Power supply interruption" event
- "Motion data error" event
- "Security breach attempt" event
- "Card" fault
- "Recording equipment" fault includes
  - internal fault
  - Printer fault
  - Display fault
  - Downloading fault
  - motion sensor fault

Additional specific faults (e.g. CAN-transmission-fault) are also detected and stored in the TOE.

## (10) built-in and self tests

The TOE is provided with the capacity to detect automatically system malfunctions related to firmware, external data memory, chipcard interfaces, downloading and the motion sensor.

## (11) reading from data memory

The TOE is able to read any data stored in its external data memory.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					10 / 52



# SECURITY TARGET DTCO 1381, Release 1.3v

## *(12) recording and storing in data memory*

The external data memory is used for recording all activities of both drivers (1 and 2) and the vehicle over a period of 365 calendar days under the assumptions of Annex I (B) <sup>2</sup>.

The TOE is able to record and store the following data: (see O1 to O18).

## *(13) reading from tachograph cards*

The TOE is able to read from tachograph cards the necessary data related to the functional requirements.

## *(14) recording and storing in tachograph cards*

The TOE is able to record and store in tachograph cards the necessary data related to the functional requirements.

## *(15) displaying*

The display is a LC display. There may be shown on the display different display menus and data.

## *(16) printing*

The TOE incorporates a thermo-printer. The paper roll can be changed. The printouts can be selected and activated by use of display and operator keys.

## *(17) warning*

The TOE warns the user when detecting any event and/or fault. It also warns the driver 15 minutes before and at the time of exceeding 4 h:30 min. continuous driving time. The warnings are visualised by the use of pictograms combined with text announcement and by the use of the display.

## *(18) data downloading to external media*

The calibration-/downloading connector on the front is used for the downloading of the external data memory or a driver card contents during control, calibration and company mode. The TOE provides the downloading through its calibration-/ downloading interface.

## *(19) output data to additional external devices*


The TOE is able to output data ( e.g. speed and distance) to instrument clusters and to the vehicle. Other data can be output to other components via the vehicle connectors. The TOE is able to output data (e.g. driver activities) via a separated info-interface (external interface).

## *(20) calibration*

The front calibration-/downloading connector is used for the calibration of the necessary parameters (w-factor, odometer, VIN etc. ). The TOE provides the calibration through its calibration-/ downloading interface.

Furthermore, the functions of the equipment and the measuring of the signals are checked during periodic inspection (every 2 years) via this connector.

For calibration and measuring via this connector approved tools (e.g. the MTC mobile test computer) will be available.

Designed by		Date	Department	Released by	Date	Department
				Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
		Designation Security Target DTCO 1381, Release 1.3				
		Document 40225345 SPE 000 AA			Version	Pages
						11 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

The calibration in calibration mode is also possible via K-line-diagnostic and CAN interface.

## (21) time adjustment

The time adjustment function in the TOE allows the user to adjust the current time in amounts of 1 minute maximum at intervals of not less than 7 days. Only in calibration mode this function is without limitation.

## (22) Software upgrade

The software upgrade is only possible in the calibration mode of the TOE. The TOE application transfers the control to the software upgrade modul (SWUM). The SWUM controls all resources of the TOE and manages the whole cycle. After the software upgrade the SWUM gives back the control to the TOE. application.

## (23) Remote Download

It is possible to authenticate a company card via external interfaces (CAN-Diagnostic, K-Line-Diagnostic over the front calibration-/downloading connector). This company card is inserted in a personal computer connected with a dedicated application (with a card reader) in the company office.

A remote download is carried out according to the following procedure:

- Identification and Authentication of a company card over the above mentioned external interfaces.
- Transfer of a download list (including all required download data blocks)
- Download of the data blocks of the download list in a specified period

### 5.1.3 Power saving mode of the TOE

A power saving mode is implemented as an additional, optional feature. It is only used by vehicle manufacturers, which need this feature. In this case the TOE is programmed at the Vehicle Unit manufacturer site to enable the power saving mode.

In the power saving mode the microcontroller changes its state between normal running and the so called interruptible power down mode in which nearly the whole microcontroller is switched off and only some interrupts remain enabled, to wake up the microcontroller.

By one of this interrupt-inputs the controller is cyclically waked up by a signal, generated by the real time clock RTC. It then works out all of its normal functions and afterwards enters the power down mode again.


When the TOE is in the power saving mode, the display is switched off.

The power saving mode is only entered, when specific conditions are fulfilled.

The power saving mode is ended and the display is switched on, if one of these specific conditions for the entrance into this mode is no more fulfilled.

Some events make it necessary respectively useful to wake up the microcontroller directly by an interrupt and not to wait for the cyclic interrupt of the RTC.

These interrupt sources are separate inputs of the controller. So the reason for the wake up can be detected in the program.

Designed by		Date	Department	Released by	Date	Department	
				Winfried Rogenz	2007-11-14	SV CV Div TCO LRH	
		Designation					
		Security Target DTCO 1381, Release 1.3					
		Document				Version	Pages
		40225345 SPE 000 AA					12 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

All of the functions of the program of the TOE are performed too in the power saving mode with some exceptions.

## 5.1.4 Manuals

For the TOE exist the following manuals:

### Operating instructions:

- |   |  |
|---|--|
| for drivers /co-drivers and haulage company | as a specification which gives the operating instructions for the driver/co-driver for normal usage and informs the driver/co-driver about the behaviour of the TOE<br>as a specification to inform the staff of the haulage company about the behaviour of the TOE and gives the operating instructions for the staff of the haulage company for normal usage of the TOE by the company (company lock, data downloading, etc.). |
| for control officers                        | as a specification to inform the control officers about the behaviour of the TOE and gives the operating instructions for the national control authorities for normal usage of the TOE by control officers (data downloading, over speeding control, etc.).  |

### Technical product manual

This manual contains a description of the process to

- install the TOE into the vehicle,
- activate the TOE,
- pair the TOE with the motion sensor,
- calibrate the TOE (with the description of default parameters) and
- carry out the periodic inspection of the TOE.

Technical description "software upgrade"

- upgrade of the software in the TOE,

These manuals are the guidance documents for authorised workshop staff, fitters and vehicle manufacturers.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					13 / 52



5.2 Vehicle Unit life cycle

The typical life cycle of the VU is described in the following figure:

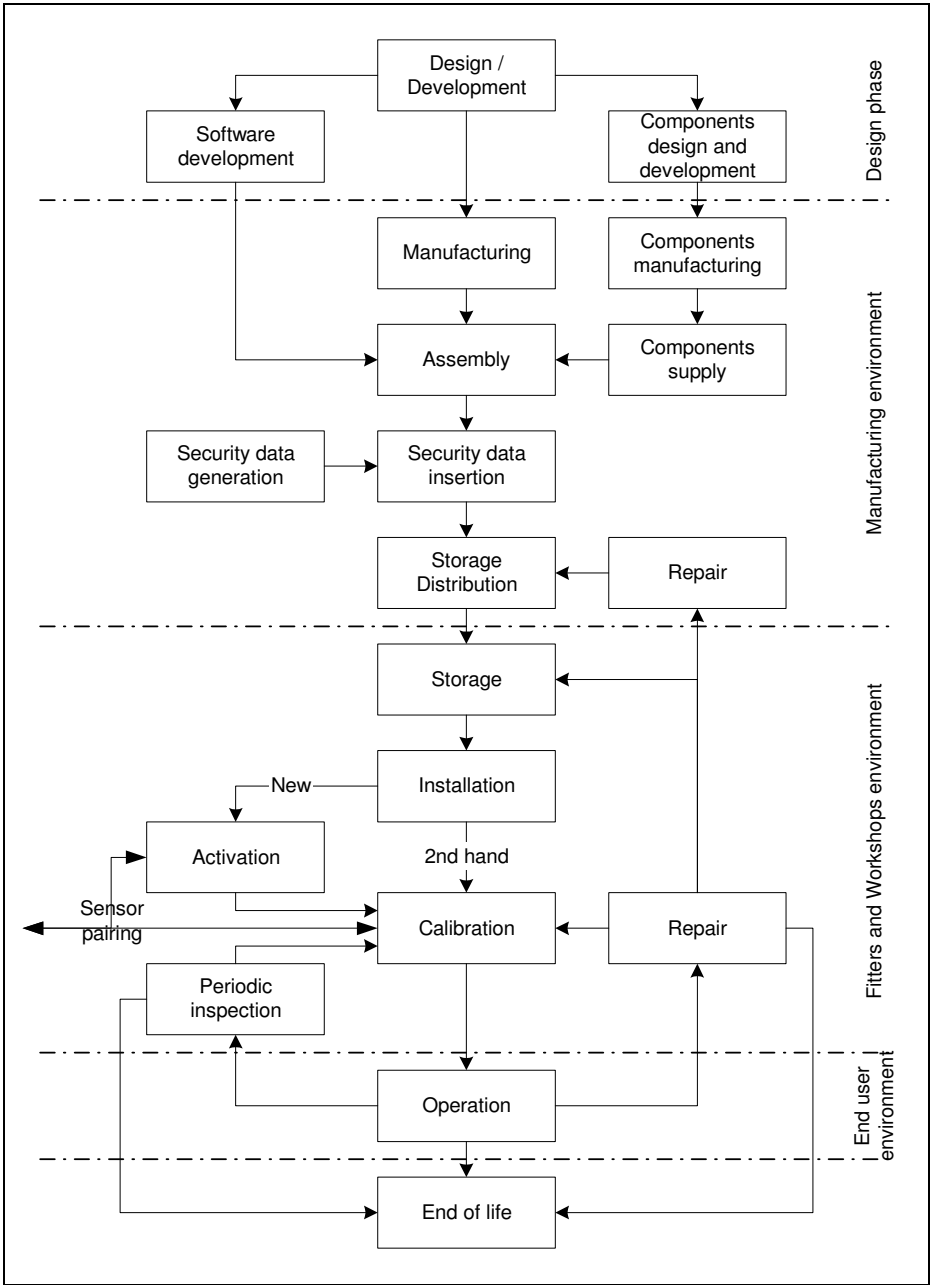


Figure 4 VU typical life cycle

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					14 / 52



Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

5.2.1 Implementation in the TOE

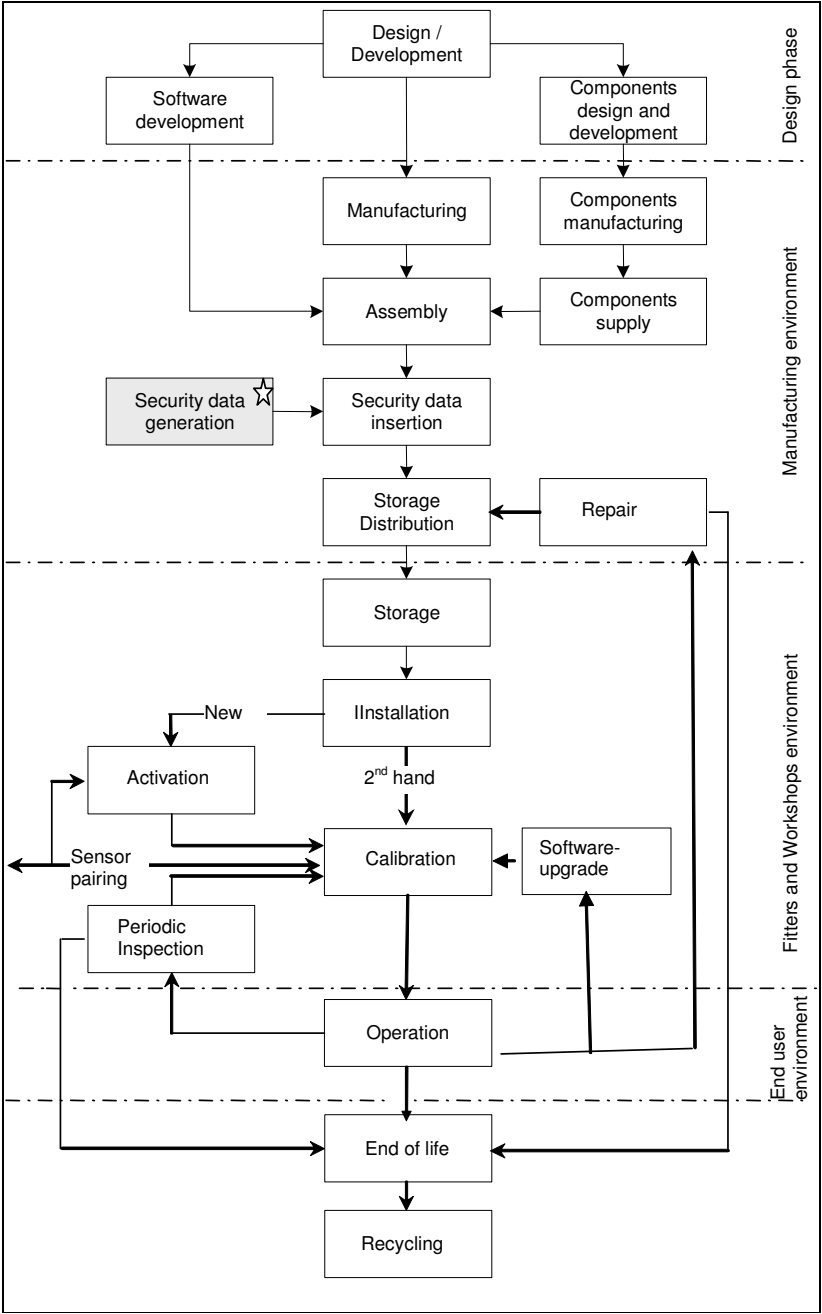


Figure 5 Life Cycle of the TOE DTCO 1381

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA				Version	Pages
					15 / 52

Qt: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

# SECURITY TARGET DTCO 1381, Release 1.3v

For the TOE a repair in the fitters and workshop environments isn't planned. Fitters or workshops can only change elements of the TOE as e.g. front covers, printer....

\* Note: The security data generation is performed in a trusted environment in the production and the keys will be certified by the National Certification Authority.

## 5.3 Subjects, objects, and access rights

### 5.3.1 Subjects

For the TOE the following types of **subjects** exist:

#### **S1 entities:**

S1.1 installation device in the manufacturing process for storing objects O1, O2, O18 in the external data memory of the TOE

S1.2 motion sensor in pairing and operational mode

S1.3 calibration device (programming tools)

S1.4 intelligent dedicated equipment for downloading (e.g. personal computer)

S1.5 tachograph cards

S1.6 management device

#### **S2 users:**

S2.1 drivers and co-drivers (in operational mode)

S2.2 workshop staff , fitters and staff of vehicle manufacturers (in calibration mode)

S2.3 control officers from national control authorities (in control mode)

S2.4 staff of the respective haulage company (in company mode)

S2.5 unknown

**Note:** The human users S2.1 to S2.4 of the recording equipment in road transport vehicles identify themselves to the TOE using tachograph cards. Authentication and access control for those users is performed by TOE unit by identifying the type of tachograph cards.

### 5.3.2 Objects

For the specification of the security functions of the TOE the following **objects** are relevant. Definitions of data objects are provided in the Appendix 1<sup>5</sup> of Annex IB.


#### **O1 equipment identification data**

O1.1 vehicle unit identification data

O1.2 motion sensor identification data

#### **O2 security elements to be stored in the TOE**

O2.1 european public key EUR.PK

Designed by		Date	Department	Released by	Date	Department	
				Winfried Rogenz	2007-11-14	SV CV Div TCO LRH	
		Designation					
		Security Target DTCO 1381, Release 1.3					
		Document				Version	Pages
		40225345 SPE 000 AA					16 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

O2.2 member State certificate  $MS_i.C$

O2.3 equipment certificate  $EQT_j.C$  includes equipment public key  $EQT_j.PK$

O2.4 equipment private key  $EQT_j.SK$

O2.5 part of the Master key  $Km_{vu}$

O2.6 security device public key  $SECDEV.PK$

## **O3 security elements to generate and to be stored in the TOE**

O3.1 session key between motion sensor and vehicle unit  $K_{sm}$

O3.2 session key between tachograph cards and vehicle unit  $K_{st}$

## **O4 driver card insertion and withdrawal data**

## **O5 driver activity data**

## **O6 places where daily work periods start and/or end**

## **O7 odometer data**

## **O8 detailed speed data**

## **O9 events data**

O9.1 card conflict

O9.2 driving without an appropriate card

O9.3 card insertion while driving

O9.4 last card session not correctly closed

O9.5 over speeding

O9.6 power supply interruption

O9.7 motion data error

O9.8 security breach attempt

## **O10 faults data**

O10.1 card fault

O10.2 recording equipment faults

## **O11 calibration data**

## **O12 time adjustment data**

## **O13 control activity data**


## **O14 company locks data**

## **O15 download activity data**

## **O16 specific conditions data**

## **O17 motion data representative of vehicle's speed and distance travelled**

## **O18 individual device key $K_{id}$**

Designed by		Date	Department	Released by	Date	Department
				Winfried Rogenz	2007-11-14	SV CV Div TCO LRH
		Designation Security Target DTCO 1381, Release 1.3				
		Document 40225345 SPE 000 AA				Version Pages 17 / 52

SECURITY TARGET DTCO 1381, Release 1.3v

O19 PIN from workshop card

Ob: Observe  
Pr: Protection marks for restricting the use of documents and products  
(Di (DIN 34: 1998-01)

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2007-11-14	SV CV Div TCO LPH
Designation					
Security Target DTCO 1381, Release 1.3					
Document					
40225345 SPE 000 AA					
Version Pages					
18 / 52					
Continental					



# SECURITY TARGET DTCO 1381,Release 1.3v

## 5.3.3 Access rights

The Table 1 describes the access rights under the rules as described in chapter 6.2.

	O1.1	O1.2	O2	O3	O4	O5	O6	O7	O8	O9	O10	O11	O12	O13	O14	O15	O16	O17	O18	O19
S1.1	w (once)		w (once)																w (once)	
S1.2		W		g/u														w/r	u	
S1.3												w/r	w/r							
S1.4																r				
S1.5						r	R			r	r	r	r	r	r	r	r			u
S1.6			u																	
S2.1	r	R	u	g/u	w/r	w/r	w/r	w/r	w/r	w/r	w/r	r	r	r	r		w/r			
S2.2	r	R	u	g/u	w/r	w/r	w/r	w/r	w/r	w/r	w/r	w/r	w/r	r	r	w/r	w/r			u
S2.3	r	R	u	g/u	w/r	r	R	r	r	r	r	r	r	w/r	r	w/r	r			
S2.4	r	R	u	g/u	w/r	r	R	r	r	r	r	r	r	r	w/r	w/r	r			
S2.5						w	W	w	w	w	w						w			

r = read; w = write; g = generate, u = use

**Table 1 Access rights**

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB				Version	Pages 20 / 52



# SECURITY TARGET DTCO 1381, Release 1.3v

## 5.4 Threats

This paragraph describes the threats the VU may face.

### 5.4.1 Threats to identification and access control policies


- T.Access Users could try to access functions not allowed to them (e.g. drivers gaining access to calibration function).
- T.Identification Users could try to use several identifications or no identification.

### 5.4.2 Design related threats

- T.Faults Faults in hardware, software, communication procedures could place the VU in unforeseen conditions compromising its security.
- T.Tests The use of non invalidated test modes or of existing back doors could compromise the VU security.
- T.Design Users could try to gain illicit knowledge of design either from manufacturer's material (through theft, bribery, ...) or from reverse engineering.

### 5.4.3 Operation oriented threats

- T.Calibration\_Parameters Users could try to use mis-calibrated equipment (through calibration data modification, or through organisational weaknesses).
- T.Card\_Data\_Exchange Users could try to modify data while exchanged between VU and tachograph cards (addition, modification, deletion, replay of signal).
- T.Clock Users could try to modify internal clock.
- T.Environment Users could compromise the VU security through environmental attacks (thermal, electromagnetic, optical, chemical, mechanical,...).
- T.Fake\_Devices Users could try to connect fake devices (motion sensor, smart cards) to the VU.
- T.Hardware Users could try to modify VU hardware.
- T.Motion\_Data Users could try to modify the vehicle's motion data (addition, modification, deletion, replay of signal).
- T.Non\_Activated Users could use non activated equipment.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version Pages
					21 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pri: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

T.Output_Data	Users could try to modify data output (print, display or download).
T.Power_Supply	Users could try to defeat the VU security objectives by modifying (cutting, reducing, increasing) its power supply.
T.Security_Data	Users could try to gain illicit knowledge of security data during security data generation or transport or storage in the equipment.
T.Software	Users could try to modify VU software.
T.Stored_Data	Users could try to modify stored data (security or user data).

## 5.5 Security objectives

The main security objective of the digital tachograph system is the following:

O.Main	The data to be checked by control authorities must be available and reflect fully and accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.
--------	--

Therefore the security objectives of the VU, contributing to the global security objective, are the following:


O.VU_Main	The data to be measured and recorded and then to be checked by control authorities must be available and reflect accurately the activities of controlled drivers and vehicles in terms of driving, work, availability and rest periods and in terms of vehicle speed.
O.VU_Export	The VU must be able to export data to external storage media in such a way as to allow for verification of their integrity and authenticity.

## 5.6 Information Technology Security Objectives

The specific IT security objectives of the VU contributing to its main security objective, are the following:

O.Access	The VU must control user access to functions and data.
O.Accountability	The VU must collect accurate accountability data.
O.Audit	The VU must audit attempts to undermine system security and

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 22 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

	should trace them to associated users.
O.Authentication	The VU should authenticate users and connected entities (when a trusted path needs to be established between entities).
O.Integrity	The VU must maintain stored data integrity.
O.Output	The VU must ensure that data output reflects accurately data measured or stored.
O.Processing	The VU must ensure that processing of inputs to derive user data is accurate.
O.Reliability	The VU must provide a reliable service.
O.Secured_Data_Exchange	The VU must secure data exchanges with the motion sensor and with tachograph cards.

## 5.7 Physical, personnel or procedural means

This paragraph describes physical, personnel or procedural requirements that contribute to the security of the VU.


### 5.7.1 Equipment design

M.Development	VU developers must ensure that the assignment of responsibilities during development is done in a manner which maintains IT security.
M.Manufacturing	VU manufacturers must ensure that the assignment of responsibilities during manufacturing is done in a manner which maintains IT security, and that during the manufacturing process the VU is protected from physical attacks which might compromise IT security.

### 5.7.2 Equipment delivery and activation

M.Delivery	VU manufacturers, vehicle manufacturers and fitters or workshops must ensure that handling of the VU is done in a manner which maintains IT security.
M.Activation	Vehicle manufacturers and fitters or workshops must activate the VU after its installation before the vehicle leaves the premises where installation took place.

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 23 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pri: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

## 5.7.3 Security data generation and delivery

M.Sec_Data_Generation	Security data generation algorithms must be accessible to authorised and trusted persons only. They must be cryptographic strong.
M.Sec_Data_Transport	Security data must be generated, transported, and inserted into the VU, in such a way to preserve its appropriate confidentiality and integrity.
M.Sec_Data_Crypt	Security data inserted into the VU must be cryptographic strong.

## 5.7.4 Cards delivery

M.Card_Availability	Tachograph cards must be available and delivered to authorised persons only.
M.Driver_Card_Uniqueness	Drivers must possess, at one time, one valid driver card only.
M.Card_Traceability	Card delivery must be traceable (white lists, black lists) , and black lists must be used during security audits.

## 5.7.5 Recording equipment installation, calibration, and inspection

M.Approved_Workshops	Installation, calibration and repair of recording equipment must be carried by trusted and approved fitters or workshops.
M.Regular_Inspections	Recording equipment must be periodically inspected and calibrated.
M.Faithful_Calibration	Approved fitters and workshops must enter proper vehicle parameters in recording equipment during calibration.

## 5.7.6 Equipment operation

M.Faithful_Drivers	Drivers must play by the rules and act responsibly (e.g. use their driver cards, properly select their activity for those that are manually selected, ...).
--------------------	---


## 5.7.7 Law enforcement control

M.Controls	Law enforcement controls must be performed regularly and randomly, and must include security audits.
------------	--

## 5.7.8 Software upgrades

M.Software_Upgrade	Software revisions must be granted security certification before they can be implemented in a VU.
--------------------	---

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.


Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 24 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pri: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

- The Management Device (MD) is installed in the approved workshops according to M.Approved\_Workshops.
- The software update data and necessary key data (for the software update) are imported into the MD by the approved workshops according to M.Approved\_Workshops.
- The Management Device supports the appropriate communication interface with the Digital Tachograph and secures the relevant secrets inside the MD as appropriate.

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
Document			Version		Pages
40225345 SPE 000 AB					25 / 52

## 6.1 Identification and authentication

This SEF includes the following features:


**UIA\_201** The VU shall be able to establish, for every interaction, the identity of the motion sensor it is connected to.

*UIA\_203* The VU shall authenticate the motion sensor it is connected to:

- Authentication shall be mutual and triggered by the VU.

UIA_205	The VU shall detect and prevent use of authentication data that has been copied and replayed.
---------	---


- generate an audit record of the event,
- warn the user,
- continue to accept and use non secured motion data sent by the motion sensor.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version 26 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.1.2 User identification and authentication

- UIA\_207* The VU shall permanently and selectively track the identity of two users, by monitoring the tachograph cards inserted in respectively the driver slot and the co-driver slot of the equipment.
- UIA\_208* The user identity shall consist of:
- a user group:
    - DRIVER (driver card),
    - CONTROLLER (control card),
    - WORKSHOP (workshop card),
    - COMPANY (company card),
    - UNKNOWN (no card inserted),
  - a user ID, composed of :
    - the card issuing Member State code and of the card number,
    - UNKNOWN if user group is UNKNOWN.
- UNKNOWN identities may be implicitly or explicitly known.
- UIA\_209* The VU shall authenticate its users at card insertion.
- UIA\_210* The VU shall re-authenticate its users:
- At power supply recovery,
  - periodically or after occurrence of specific events (*TBD by manufacturers: every 12 hours and more frequently than once per day*).
- UIA\_211* Authentication shall be performed by means of proving that the card inserted is a valid tachograph card, possessing security data that only the system could distribute. Authentication shall be mutual and triggered by the VU.
- UIA\_212* In addition to the above, workshops shall be required to be successfully authenticated through a PIN check. PIN's shall be at least 4 characters long.
- Note: In the case the PIN is transferred to the VU from an outside equipment located in the vicinity of the VU, PIN confidentiality need not be protected during the transfer.
- UIA\_213* The VU shall detect and prevent use of authentication data that has been copied and replayed.
- UIA\_214* After 5 consecutive unsuccessful authentication attempts have been detected, the SEF shall:
- generate an audit record of the event,
  - warn the user,
  - assume the user as UNKNOWN, and the card as non valid (definition z) and requirement 007).

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 27 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

## definition z in <sup>2</sup>

“non valid card” means:

a card detected as faulty, or which initial authentication failed, or which start of validity date is not yet reached, or which expiry date has passed.

## requirement 007/008 in <sup>2</sup>

The recording equipment shall switch to the following mode of operation according to the valid tachograph cards inserted into the card interface devices:

Mode of operation		Driver slot				
		No card	Driver card	Control card	Workshop card	Company card
Co-driver slot	No card	Operational	Operational	Control	Calibration	Company
	Driver card	Operational	Operational	Control	Calibration	Company
	Control card	Control	Control	Control <sup>(*)</sup>	Operational	Operational
	Workshop card	Calibration	Calibration	Operational	Calibration <sup>(*)</sup>	Operational
	Company card	Company	Company	Operational	Operational	Company <sup>(*)</sup>


<sup>(\*)</sup> In these situations the recording equipment shall use only the tachograph card inserted in the driver slot.

### 6.1.3 Remotely connected company identification and authentication

Company remote connection capability is implemented.

- UIA\_215** For every interaction with a remotely connected company, the VU shall be able to establish the company's identity.
- UIA\_216** The remotely connected company's identity shall consist of its company card issuing Member State code and of its company card number.
- UIA\_217** The VU shall successfully authenticate the remotely connected company before allowing any data export to it.
- UIA\_218** Authentication shall be performed by means of proving that the company owns a valid company card, possessing security data that only the system could distribute.
- UIA\_219** The VU shall detect and prevent use of authentication data that has been copied and replayed.
- UIA\_220** After 5 consecutive unsuccessful authentication attempts have been detected, the VU shall:

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by		Date	Department	Released by	Date	Department
				Winfried Rogenz	2012-04-25	I CV AM TTS LRH
		Designation Security Target DTCO 1381, Release 1.3v				
		Document 40225345 SPE 000 AB				Version 28 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

- warn the remotely connected company.

## 6.1.4 Management device identification and authentication

VU manufacturers may foresee dedicated devices for additional VU management functions (e.g. Software upgrading, security data reloading, ...). This paragraph therefore applies only if this feature is implemented.

A dedicated management device is foreseen for the software upgrade of the TOE.

- UIA\_221** For every interaction with a management device, the VU shall be able to establish the device identity.
- UIA\_222** Before allowing any further interaction, the VU shall successfully authenticate the management device.
- UIA\_223** The VU shall detect and prevent use of authentication data that has been copied and replayed.

## 6.2 Access control

Access controls ensure that information is read from, created in, or modified into the TOE only by those authorised to do so.


It must be noted that the user data recorded by the VU, although presenting privacy or commercial sensitivity aspects, are not of a confidential nature. Therefore, the functional requirement related to data read access rights (requirement 011) is not the subject of a security enforcing function.

### Requirement 011 of Annex 1B:

*The recording equipment can output any data to display, printer or external interfaces with the following exceptions:*

- *in the operational mode, any personal identification (surname and first name(s)) not corresponding to a tachograph card inserted shall be blanked and any card number not corresponding to a tachograph card inserted shall be partially blanked (every odd character shall be blanked),*
- *in the company mode, driver related data can be output only for periods not locked by another company (as identified by the first 13 digits of the company card number),*
- *when no card is inserted in the recording equipment, driver related data can be output only for the current and 8 previous calendar days.*

**<SEF2>** The TOE provides this security enforcing function of access control for access to function and data of the TOE.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 29 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

This SEF includes the following features:

## 6.2.1 Access control policy

*ACC\_201* The VU shall manage and check access control rights to functions and to data.

## 6.2.2 Access rights to functions

*ACC\_202* The VU shall enforce the mode of operation selection rules (requirements 006 to 009).

### requirement 006 in <sup>2</sup> :

*The recording equipment shall possess four modes of operation:*

- *operational mode,*
- *control mode,*
- *calibration mode,*
- *company mode.*

### requirement 007/008 in <sup>2</sup> :

*see chapter 6.1.2 security enforcing function UIA\_214*

### requirement 009 in <sup>2</sup> :

*The recording equipment shall ignore non valid cards inserted, except displaying, printing or downloading data held on an expired card which shall be possible.*

*ACC\_203* The VU shall use the mode of operation to enforce the functions access control rules (requirement 010).

### requirement 010 in 2 (the functions in the TOE as described in 5.1.2 are the same as listed in II.2):

*All functions listed in II.2. shall work in any mode of operation with the following exceptions:*


- *the calibration function is accessible in the calibration mode only,*
- *the time adjustment function is limited when not in the calibration mode,*
- *the driver manual entries function are accessible in operational or calibration modes only,*
- *the company locks management function is accessible in the company mode only,*
- *the monitoring of control activities function is operational in the control mode only,*
- *the downloading function is not accessible in the operational mode.*

## 6.2.3 Access rights to data

*ACC\_204* The VU shall enforce the VU identification data write access rules (requirement 076)

### requirement 076 in <sup>2</sup> :

*Vehicle unit identification data are recorded and stored once and for all by the vehicle unit manu-*

Designed by	Date	Department	Released by	Date	Department	
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH	
	Designation Security Target DTCO 1381, Release 1.3v					
	Document				Version	Pages
	40225345 SPE 000 AB					30 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

*facturer, except the software related data and the approval number which may be changed in case of software upgrade.*

ACC\_205 The VU shall enforce the paired motion sensor identification data write access rules (requirements 079 and 155)

## requirement 079 in <sup>2</sup>:

*The vehicle unit shall be able to record and store in its data memory the following currently paired motion sensor identification data:*

- serial number,
- approval number,
- first pairing date,

## requirement 155 in <sup>2</sup>:

*Pairing the motion sensor to the VU shall consist, at least, in:*

- updating motion sensor installation data held by the motion sensor (as needed),
- copying from the motion sensor to the VU data memory necessary motion sensor identification data.

ACC\_206 After the VU activation, the VU shall ensure that only in calibration mode, may calibration data be input into the VU and stored into its data memory (requirements 154 and 156).

## requirement 154 in <sup>2</sup>:

*The calibration function shall allow:*

- to automatically pair the motion sensor with the VU,
- to digitally adapt the constant of the recording equipment ( $k$ ) to the characteristic coefficient of the vehicle ( $w$ ) (vehicles with two or more axle ratios shall be fitted with a switch device whereby these various ratios will automatically be brought into line with the ratio for which the equipment has been adapted to the vehicle),
- to adjust (without limitation) the current time,
- to adjust the current odometer value,
- to update motion sensor identification data stored in the data memory,
- to update or confirm other parameters known to the recording equipment: vehicle identification,  $w$ ,  $l$ , tyre type and speed limiting device setting if applicable.


## requirement 156 in <sup>2</sup>:

*The calibration function shall be able to input necessary data through the calibration/downloading connector in accordance with the calibration protocol defined in Appendix 8. The calibration function may also input necessary data through other connectors.*

ACC\_207 After the VU activation, the VU shall enforce calibration data write and delete access rules (requirement 097).

## requirement 097 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory data relevant to:*

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
		Document			Version Pages
		40225345 SPE 000 AB			31 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

- *known calibration parameters at the moment of activation,*
- *its very first calibration following its activation,*
- *its first calibration in the current vehicle (as identified by its VIN),*
- *the 5 most recent calibrations (If several calibrations happen within one calendar day, only the last one of the day shall be stored).*

ACC\_208 After the VU activation, the VU shall ensure that only in calibration mode, may time adjustment data be input into the VU and stored into its data memory (This requirement does not apply to small time adjustments allowed by requirements 157 and 158).

requirement 157 in <sup>2</sup>:

*The time adjustment function shall allow for adjusting the current time in amounts of 1 minute maximum at intervals of not less than 7 days.*

requirement 158 in <sup>2</sup>:

*The time adjustment function shall allow for adjusting the current time without limitation, in calibration mode.*

ACC\_209 After the VU activation, the VU shall enforce time adjustment data write and delete access rules (requirement 100).

requirement 100 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory data relevant to:*

- *the most recent time adjustment,*
  - *the 5 largest time adjustments, since last calibration,*
- performed in calibration mode outside the frame of a full calibration.*


ACC\_210 The VU shall enforce appropriate read and write access rights to security data (requirement 080).

requirement 080 in <sup>2</sup>:

*The recording equipment shall be able to store the following security elements:*

- *European public key,*
- *Member State certificate,*
- *Equipment certificate,*
- *Equipment private key.*

*Recording equipment security elements are inserted in the equipment by the vehicle unit manufacturer.*

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 32 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.2.4 File structure and access conditions

**ACC\_211** Application and data files structure and access conditions shall be created during the manufacturing process, and then locked from any future modification or deletion.

## 6.3 Accountability

**<SEF3>** The TOE provides this security enforcing function of accountability for collection of accurate data in the TOE.

This SEF includes the following features:

**ACT\_201** The VU shall ensure that drivers are accountable for their activities (requirements 081, 084, 087 105a, 105b 109 and 109a).

### requirement 081 in <sup>2</sup>:

*For each insertion and withdrawal cycle of a driver or workshop card in the equipment, the recording equipment shall record and store in its data memory:*


- the card holder's name and first names as stored in the card,
- the card's number, issuing Member State and expiry date as stored in the card,
- the insertion date and time,
- the vehicle odometer value at card insertion,
- the slot in which the card is inserted,
- the withdrawal date and time,
- the vehicle odometer value at card withdrawal,
- the following information about the previous vehicle used by the driver, as stored in the card:
  - VRN and registering Member State,
  - card withdrawal date and time;
- a flag indicating whether, at card insertion, the card holder has manually entered activities or not.

### requirement 084 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory whenever there is a change of activity for the driver and/or the co-driver, and/or whenever there is a change of driving status, and/or whenever there is an insertion or withdrawal of a driver or workshop card:*

- the driving status (CREW, SINGLE)
- the slot (DRIVER, CO-DRIVER),
- the card status in the relevant slot (INSERTED, NOT INSERTED)(See Note),
- the activity (DRIVING, AVAILABILITY, WORK, BREAK/REST).
- the date and time of the change,

**Note:** INSERTED means that a valid driver or workshop card is inserted in the slot. NOT INSERTED means the opposite i.e. no valid driver or workshop card is inserted in the slot (e.g. a company card is inserted or no card is inserted)

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 33 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## requirement 087 in <sup>2</sup>:

The recording equipment shall record and store in its data memory whenever a (co-) driver enters the place where a daily work period begins and/or ends:

- If applicable, the (co-)driver card number and card issuing Member State,
- the date and time of the entry,
- the type of entry (begin or end),
- the country and region entered,
- the vehicle odometer value.

## requirement 105a in <sup>2</sup>:

The recording equipment shall record in its data memory the following data relevant to specific conditions:

- Date and time of the entry,
- Type of specific condition.

## requirement 105b in <sup>2</sup>:

The data memory shall be able to hold specific conditions data for at least 365 days (with the assumption that on average, 1 condition is opened and closed per day). When storage capacity is exhausted, new data shall replace oldest data.

## requirement 109 in <sup>2</sup>:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

## requirement 109a in <sup>2</sup>:


The recording equipment shall update driver activity data (as specified in Chapter IV paragraph 5.2.5), stored on valid driver and/or workshop cards, with activity data manually entered by the cardholder.

ACT\_202 The VU shall hold permanent identification data (requirement 075).

## requirement 075 in <sup>2</sup>:

The recording equipment shall be able to store in its data memory the following vehicle unit identification data:

- name of the manufacturer,
- address of the manufacturer,
- part number,
- serial number,
- software version number,
- software version installation date,
- year of equipment manufacture,
- approval number,

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 34 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

ACT\_203 The VU shall ensure that workshops are accountable for their activities (requirements 098, 101 and 109).

## requirement 098 in <sup>2</sup>:

*The following data shall be recorded for each of these calibrations:*

- Purpose of calibration (activation, first installation, installation, periodic inspection, other)
- workshop name and address,
- workshop card number, card issuing Member State and card expiry date,
- vehicle identification,
- parameters updated or confirmed: w, k, l, tyre type, speed limiting device setting, odometer (old and new values), date and time (old and new values).

## requirement 101 in <sup>2</sup>:

*The following data shall be recorded for each of these time adjustments:*

- date and time, old value,
- date and time, new value,
- workshop name and address,
- workshop card number, card issuing Member State and card expiry date.

## requirement 109 in <sup>2</sup>:

*The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.*

ACT\_204 The VU shall ensure that controllers are accountable for their activities (requirements 102, 103 and 109).

## requirement 102 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent control activities:*


- date and time of the control,
- control card number and card issuing Member State,
- type of the control (displaying and/or printing and/or VU downloading and/or card downloading).

## requirement 103 in <sup>2</sup>:

*In case of downloading, the dates of the oldest and of the most recent days downloaded shall also be recorded.*

## requirement 109 in <sup>2</sup>:

*The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.*

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 35 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

ACT\_205 The VU shall record odometer data (requirement 090) and detailed speed data (requirement 093).

requirement 090 in <sup>2</sup>:

*The data memory shall be able to store midnight odometer values for at least 365 calendar days.*

requirement 093 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory the instantaneous speed of the vehicle and the corresponding date and time for every second of at least the last 24 hours that the vehicle has been moving.*

ACT\_206 The VU shall ensure that user data related to requirements 081 to 093 and 102 to 105b inclusive are not modified once recorded, except when becoming oldest stored data to be replaced by new data.

requirement 081 to 083 in <sup>2</sup>:

*Driver card insertion and withdrawal data*

requirement 084 to 086 in <sup>2</sup>:

*Driver activity data*

requirement 087 to 089 in <sup>2</sup>:

*Places where daily work periods start and/or end*

requirement 090 to 092 in <sup>2</sup>:

*Odometer data*

requirement 093 in <sup>2</sup>:

*Detailed speed data*

requirement 102 to 103 in <sup>2</sup>:

*Control activity data*

requirement 104 in <sup>2</sup>:

*Company locks data*

requirement 105 in <sup>2</sup>:

*Download activity data*

ACT\_207 The VU shall ensure that it does not modify data already stored in a tachograph card (requirement 109 and 109a) except for replacing oldest data by new data (requirement 110) or in the case described in Appendix 1 Paragraph 2.1.Note.

requirement 109 in <sup>2</sup>:


*The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.*

requirement 109a in <sup>2</sup>:

*see ACT\_201*

requirement 110 in <sup>2</sup>:

*Tachograph cards data update shall be such that, when needed and taking into account card actual storage capacity, most recent data replace oldest data.*

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 36 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.4 Audit

Audit capabilities are required only for events that may indicate a manipulation or a security breach attempt. It is not required for the normal exercising of rights even if relevant to security.

**<SEF4>** The TOE provides this security enforcing function of audit related to attempts to undermine the security of the TOE and provides the traceability to associated users.

This SEF includes the following features:


**Note:** The security breach attempt "internal data transfer" does not apply to the TOE, because it does not make use of physically separated parts (see 6.6.2.).

**AUD\_201** The VU shall, for events impairing the security of the VU, record those events with associated data (requirements 094, 096 and 109).

requirement 094 in <sup>2</sup>:

*The recording equipment shall record and store in its data memory the following data for each event detected according to the following storage rules:*

Event	Storage rules	Data to be recorded per event
Card conflict	- the 10 most recent events.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Member State of the two cards creating the conflict.
Driving without an appropriate card	- the longest event for each of the 10 last days of occurrence, - the 5 longest events over the last 365 days.	- date and time of beginning of event, - date and time of end of event, - cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event, - number of similar events that day.
Card insertion while driving	- the last event for each of the 10 last days of occurrence,	- date and time of the event, - card's type, number and issuing Member State, - number of similar events that day
Last card session not correctly closed	- the 10 most recent events.	- date and time of card insertion, - card's type, number and issuing Member State, - last session data as read from the card: - date and time of card insertion, - VRN and Member State of registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 37 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Over speed-ing (1)	<ul style="list-style-type: none"> <li>- the most serious event for each of the 10 last days of occurrence (i.e. the one with the highest average speed),</li> <li>- the 5 most serious events over the last 365 days.</li> <li>- the first event having occurred after the last calibration</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of event,</li> <li>- date and time of end of event,</li> <li>- maximum speed measured during the event,</li> <li>- arithmetic average speed measured during the event,</li> <li>- card's type, number and issuing Member State of the driver (if applicable),</li> <li>- number of similar events that day.</li> </ul>
Power supply interrup-tion (2)	<ul style="list-style-type: none"> <li>- the longest event for each of the 10 last days of occurrence,</li> <li>- the 5 longest events over the last 365 days.</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of event,</li> <li>- date and time of end of event,</li> <li>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,</li> <li>- number of similar events that day.</li> </ul>
Motion data error	<ul style="list-style-type: none"> <li>- the longest event for each of the 10 last days of occurrence,</li> <li>- the 5 longest events over the last 365 days.</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of event,</li> <li>- date and time of end of event,</li> <li>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,</li> <li>- number of similar events that day.</li> </ul>
Security breach attempt	<ul style="list-style-type: none"> <li>- the 10 most recent events per type of event.</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of event,</li> <li>- date and time of end of event (if relevant),</li> <li>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the event,</li> <li>- type of event.</li> </ul>


## requirement 096 in <sup>2</sup>:

The recording equipment shall attempt to record and store in its data memory the following data for each fault detected according to the following storage rules:

<b>Fault</b>	<b>Storage rules</b>	<b>Data to be recorded per fault</b>
Card fault	<ul style="list-style-type: none"> <li>- the 10 most recent driver card faults.</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of fault,</li> <li>- date and time of end of fault,</li> <li>- card's type number and issuing Member State.</li> </ul>
Re-cording equip-ment faults	<ul style="list-style-type: none"> <li>- the 10 most recent faults for each type of fault,</li> <li>- the first fault after the last calibration.</li> </ul>	<ul style="list-style-type: none"> <li>- date and time of beginning of fault,</li> <li>- date and time of end of fault,</li> <li>- type of fault,</li> <li>- cards' type, number and issuing Member State of any card inserted at beginning and/or end of the fault.</li> </ul>

## requirement 109 in <sup>2</sup>:

The recording equipment shall update data stored on valid driver, workshop and/or control cards with all necessary data relevant to the period while the card is inserted and relevant to the card holder. Data stored on these cards are specified in Chapter IV.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
		Document	Version		
		40225345 SPE 000 AB	Pages		
			38 / 52		

# SECURITY TARGET DTCO 1381, Release 1.3v

**AUD\_202** The events affecting the security of the VU are the following:

- Security breach attempts:
  - motion sensor authentication failure,
  - tachograph card authentication failure,
  - unauthorised change of motion sensor,
  - card data input integrity error,
  - stored user data integrity error,
  - internal data transfer error,
  - unauthorised case opening,
  - hardware sabotage,
- Last card session not correctly closed,
- Motion data error event,
- Power supply interruption event,
- VU internal fault.

**AUD\_203** The VU shall enforce audit records storage rules (requirement 094 and 096).

requirement 094 in <sup>2</sup>:

*see security enforcing function AUD\_201*

requirement 096 in <sup>2</sup>:

*see security enforcing function AUD\_201*

**AUD\_204** The VU shall store audit records generated by the motion sensor in its data memory.


**AUD\_205** It shall be possible to print, display and download audit records.

## 6.5 Object re-use

**<SEF5>** The TOE provides this security enforcing function of object reuse.

This SEF includes the following features:

**REU\_201** The VU shall ensure that temporary storage objects can be reused without this involving inadmissible information flow.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
Document			Version	Pages	
40225345 SPE 000 AB				39 / 52	

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.6 Accuracy

<SEF6> The TOE provides this security enforcing function of accuracy of stored data in the TOE.

This SEF includes the following features:

### 6.6.1 Information flow control policy

ACR\_201 The VU shall ensure that user data related to requirements 081, 084, 087, 090, 093, 102, 104, 105, 105a and 109 may only be processed from the right input sources:

- vehicle motion data,
- VU's real time clock,
- recording equipment calibration parameters,
- tachograph cards,
- user's inputs.

requirement 081, 084, 087, 105, 105a, 109 in <sup>2</sup>:

see chapter 6.3 security enforcing function ACT\_201

requirement 102 in <sup>2</sup>:

see chapter 6.3 security enforcing function ACT\_204

requirement 090, 093 in <sup>2</sup>:

see chapter 6.3 security enforcing function ACT\_205

requirement 104 in <sup>2</sup>:

The recording equipment shall record and store in its data memory the following data relevant to the 20 most recent company locks:

- lock-in date and time,
- lock-out date and time,
- company card number and card issuing Member State,
- company name and address.


ACR\_201a The VU shall ensure that user data related to requirement 109a may only be entered for the period last card withdrawal – current insertion (requirement 050a).

requirement 109a in <sup>2</sup>:

see chapter 6.3 security enforcing function ACT\_201

requirement 50a in <sup>2</sup>:

Upon driver (or workshop) card insertion, and only at this time, the recording equipment shall remind to the cardholder the date and time of his last card withdrawal and the activity selected at that time, and shall prompt the cardholder for a "Declaration ?". If the prompt is negatively an-

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version Pages 40 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

swered, the recording equipment shall require the cardholder to confirm his answer. If the prompt is positively answered, the recording equipment shall:

- allow the cardholder to manually enter activities, with their dates and times of beginning and end, among WORK or AVAILABILITY or BREAK/REST only, strictly included within the period last card withdrawal – current insertion only,
- allow the cardholder to modify or delete any such activities manually entered, until validation by selection of a specific command, and then forbid any such modification,
- not allow entry of activities that overlap activities already entered.

A positive answer to the prompt followed by no activity entries, shall be interpreted by the recording equipment as a negative answer to the prompt.

During this process, the recording equipment shall wait for entries no longer than the following time-outs:

- if no interaction with the equipment's human machine interface is happening during 1 minute (with an audible or visual warning after 30 seconds) or,
  - if the card is withdrawn or another driver (or workshop) card is inserted or,
  - as soon as the vehicle is moving,
- in this case the recording equipment shall validate any entries already made.

## 6.6.2 Internal data transfers

The requirements of this paragraph apply only if the VU makes use of physically separated parts.

**ACR\_202** If data are transferred between physically separated parts of the VU, the data shall be protected from modification.


**ACR\_203** Upon detection of a data transfer error during an internal transfer, transmission shall be repeated and the SEF shall generate an audit record of the event.

**Since the TOE is a single protected entity, this requirement does not apply for the TOE.**

## 6.6.3 Stored data integrity

**ACR\_204** The VU shall check user data stored in the data memory for integrity errors.

**ACR\_205** Upon detection of a stored user data integrity error, the SEF shall generate an audit record.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB			Version	Pages 41 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.7 Reliability of service

<SEF7> The TOE provides this security enforcing function of reliability of service

This SEF includes the following features:

### 6.7.1 Tests

*RLB\_201* All commands, actions or test points, specific to the testing needs of the manufacturing phase of the VU shall be disabled or removed before the VU activation. It shall not be possible to restore them for later use.

*RLB\_202* The VU shall run self tests, during initial start-up, and during normal operation to verify its correct operation. The VU self tests shall include a verification of the integrity of security data and a verification of the integrity of stored executable code (if not in ROM).

*RLB\_203* Upon detection of an internal fault during self test, the SEF shall:

- generate an audit record (except in calibration mode) (VU internal fault),
- preserve the stored data integrity.

### 6.7.2 Software

*RBL\_204* There shall be no way to analyse or debug software in the field after the VU activation.

*RLB\_205* Inputs from external sources shall not be accepted as executable code.

### 6.7.3 Physical protection

*RLB\_206* If the VU is designed so that it can be opened, the VU shall detect any case opening, except in calibration mode, even without external power supply for a minimum of 6 months. In such a case, the SEF shall generate an audit record (It is acceptable that the audit record is generated and stored after power supply reconnection).


If the VU is designed so that it cannot be opened, it shall be designed such that physical tampering attempts can be easily detected (e.g. through visual inspection).

*RLB\_207* After its activation, the VU shall detect specified (*TBD by manufacturer*) hardware sabotage:.

- Manipulation of the mechanisms for the cart reader

*RLB\_208* In the case described above, the SEF shall generate an audit record and the VU shall: (*TBD by manufacturer*).

For the mechanisms of the cart reader

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
		Document	Version		Pages
		40225345 SPE 000 AB			42 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

The audit record is displayed and stored in the memory for event and faults. If possible the data will be stored on the tachograph card and than the tachograph card withdrawals.

## 6.7.4 Power supply interruptions

**RLB\_209** The VU shall detect deviations from the specified values of the power supply, including cut-off.

**RLB\_210** In the case described above, the SEF shall:

- generate an audit record (except in calibration mode),
- preserve the secure state of the VU,
- maintain the security functions, related to components or processes still operational,
- preserve the stored data integrity.

## 6.7.5 Reset conditions

**RLB\_211** In case of a power supply interruption, or if a transaction is stopped before completion, or on any other reset conditions, the VU shall be reset cleanly.

## 6.7.6 Data availability

**RLB\_212** The VU shall ensure that access to resources is obtained when required and that resources are not requested nor retained unnecessarily.

**RLB\_213** The VU must ensure that cards cannot be released before relevant data have been stored to them (requirements 015 and 016).

### requirement 015 in <sup>2</sup>:

*The recording equipment shall be so designed that the tachograph cards are locked in position on their proper insertion into the card interface devices.*

### requirement 016 in <sup>2</sup>:


*The release of tachograph cards may function only when the vehicle is stopped and after the relevant data have been stored on the cards. The release of the card shall require positive action on behalf of the release.*

**RLB\_214** In the case described above, the SEF shall generate an audit record of the event.

## 6.7.7 Multiple applications

**The VU provides only the tachograph application.**

**RLB\_215** If the VU provides applications other than the tachograph application, all applications shall be physically and/or logically separated from each other. These applications shall

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version Pages
					43 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

not share security data. Only one task shall be active at a time.

## 6.8 Data exchange

This paragraph addresses data exchange between the VU and connected devices.

**<SEF8>** The TOE provides this security enforcing function of data exchange with connected entities.

This SEF includes the following features:

### 6.8.1 Data exchange with motion sensor

*DEX\_201* The VU shall verify the integrity and authenticity of motion data imported from the motion sensor.

*DEX\_202* Upon detection of a motion data integrity or authenticity error, the SEF shall:

- generate an audit record,
- continue to use imported data.


### 6.8.2 Data exchange with tachograph cards

*DEX\_203* The VU shall verify the integrity and authenticity of data imported from tachograph cards.

*DEX\_204* Upon detection of a card data integrity or authenticity error, the SEF shall:

- generate an audit record,
- not use the data.

*DEX\_205* The VU shall export data to tachograph smart cards with associated security attributes such that the card will be able to verify its integrity and authenticity.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
Document			Version	Pages	
40225345 SPE 000 AB				44 / 52	

# SECURITY TARGET DTCO 1381, Release 1.3v

## 6.8.3 Data exchange with external storage media (downloading function))

- DEX\_206* The VU shall generate an evidence of origin for data downloaded to external media.
- DEX\_207* The VU shall provide a capability to verify the evidence of origin of downloaded data to the recipient.
- DEX\_208* The VU shall download data to external storage media with associated security attributes such that downloaded data integrity and authenticity can be verified.


## 6.9 Cryptographic support

The requirements of this paragraph are applicable only where needed, depending upon security mechanisms used and upon the manufacturer's solutions.

<SEF9> The TOE provides this security enforcing function of cryptographic support.

This SEF includes the following features:

- CSP\_201* Any cryptographic operation performed by the VU shall be in accordance with a specified algorithm and a specified key size.
- CSP\_202* If the VU generates cryptographic keys, it shall be in accordance with specified cryptographic key generation algorithms and specified cryptographic key sizes
- CSP\_203* If the VU distributes cryptographic keys, it shall be in accordance with specified key distribution methods.
- CSP\_204* If the VU accesses cryptographic keys, it shall be in accordance with specified cryptographic keys access methods.
- CSP\_205* If the VU destroys cryptographic keys, it shall be in accordance with specified cryptographic keys destruction methods.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version Pages
					45 / 52

## 7 Definition of security mechanisms

Required security mechanisms are specified in Appendix 11 <sup>6</sup>.

All other security mechanisms are to be defined by manufacturers.


The TOE provides the security mechanisms as described in the documents for the detailed design to its users and entities.

## 8 Minimum strength of security mechanisms

The minimum strength of the Vehicle Unit security mechanisms is **High**, as defined in ITSEC <sup>7</sup>.

## 9 Level of assurance

The target level of assurance for the Vehicle Unit is ITSEC level **E3**, as defined in ITSEC <sup>7</sup>.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
Document			Version	Pages	
40225345 SPE 000 AB				46 / 52	

# SECURITY TARGET DTCO 1381, Release 1.3v

## 10 Rationale

The following matrixes give a rationale for the SEFs by showing:

- which SEFs or means counteract which threats,
- which SEFs fulfil IT security objectives.

	Threats																IT Objectives											
	Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply	Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange	
	Physical Personnel Procedural Means																											
	Development			x	x	x																						
	Manufacturing				x	x																						
	Delivery													x														
	Activation	x												x														
	Security Data Generation																	x										
	Security Data Transport																	x										
	Security Data Crypt																	x										
Card Availability		x																										
One Driver Card		x																										
Card Traceability		x																										
Approved Workshops						x		x																				
Regular Inspection Calibration						x		x			x		x		x			x										
Faithful workshops						x		x																				
Faithful drivers		x														-												
Law enforcement controls		x				x		x	x		x		x		x	x	x	x										
Software Upgrade																	x	x										

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB			Version Pages 47 / 52		



# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

		Threats																IT Objectives										
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability
Security Enforcing Functions																												
<SEF1> Identification and Authentication																												
UIA_201	Sensor identification									x	x												x					x
UIA_202	Sensor identity									x	x												x					x
UIA_203	Sensor authentication									x	x												x					x
UIA_204	Sensor re-identification and re-authentication									x	x												x					x
UIA_205	Unforgeable authentication									x	x												x					
UIA_206	Authentication failure									x	x											x					x	
UIA_207	Users identification	x	x							x										x			x					x
UIA_208	User identity	x	x							x										x			x					x
UIA_209	User authentication	x	x							x										x			x					x
UIA_210	User re-authentication	x	x							x										x			x					x
UIA_211	Authentication means	x	x							x										x			x					
UIA_212	PIN checks	x	x			x		x												x			x					
UIA_213	Unforgeable authentication	x	x							x										x			x					
UIA_214	Authentication failure	x	x							x												x						
UIA_215	Remote user identification	x	x																	x			x					x
UIA_216	Remote user identity	x	x																	x			x					
UIA_217	Remote user authentication	x	x																	x			x					x
UIA_218	Authentication means	x	x																	x			x					
UIA_219	Unforgeable authentication	x	x																	x			x					
UIA_220	Authentication failure	x	x																									
UIA_221	Management device Identification	x	x																	x			x					
UIA_222	Management device Authentication	x	x																	x			x					
UIA_223	Unforgeable authentication	x	x																	x			x					

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB			Version Pages 48 / 52		




**SECURITY TARGET DTCO 1381, Release 1.3v**

Ot Observe  
Pr Protection marks for restricting the use of documents and products  
(D) (DIN 34: 1998-01)

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

		Threats															IT Objectives											
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability
<SEF2> Access Control																												
ACC_201	Access control policy	x				x	x										x	x	x									
ACC_202	Access rights to functions	x				x	x												x									
ACC_203	Access rights to functions	x				x	x													x								
ACC_204	VU ID																		x	x								
ACC_205	Connected sensor ID									x									x	x								
ACC_206	Calibration data	x				x													x	x								
ACC_207	Calibration data					x													x	x								
ACC_208	Time adjustment data	X																	x	x								
ACC_209	Time adjustment data								x										x	x								
ACC_210	Security Data																	x	x	x								
ACC_211	File structure and access conditions	x				x												x	x	x								
<SEF3> Accountability																												
ACT_201	Drivers accountability																				x							
ACT_202	VU ID data																				x	x						
ACT_203	Workshops accountability																				x							
ACT_204	Controllers accountability																				x							
ACT_205	Vehicle movement accountability																				x							
ACT_206	Accountability data modification																		x						x		x	
ACT_207	Accountability data modification																		x						x		x	
<SEF4> Audit																												
AUD_201	Audit records																						x					
AUD_202	Audit events list	x					x				x	x		x	x				x			x						
AUD_203	Audit records storage rules																					x						
AUD_204	Sensor audit records																					x						
AUD_205	Audit tools																					x						
<SEF5> Re-use																												
REU_201	Re-use																	x									x	x

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation Security Target DTCO 1381, Release 1.3v				
	Document 40225345 SPE 000 AB				Version 49 / 52

# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

		Threats															IT Objectives												
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
<SEF6> Accuracy																													
ACR_201	Information flow control policy						x			x		x															x	x	
ACR_201a	Information flow control policy						x			x		x															x	x	
ACR_202	Internal transfers														x										x	x	x		
ACR_203	Internal transfers														x							x							
ACR_204	Stored data integrity																		x					x				x	
ACR_205	Stored data integrity																		x			x							
<SEF7> Reliability																													
RLB_201	Manufacturing tests				x	x																							x
RLB_202	Self tests			x							x					x			x										x
RLB_203	Self tests										x					x			x			x							
RLB_204	Software analysis					x													x									x	
RLB_205	Software input																		x						x	x	x		
RLB_206	Case opening					x				x		x			x			x	x	x					x		x		
RLB_207	Hardware sabotage										x																	x	
RLB_208	Hardware sabotage										x											x							
RLB_209	Power supply interruptions															x												x	
RLB_210	Power supply interruptions															x							x						
RLB_211	Reset			x																								x	
RLB_212	Data Availability																									x	x		
RLB_213	Card release																											x	
RLB_214	card session not correctly closed																						x						
RLB_215	Multiple Applications																												x

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB			Version Pages 50 / 52		



# SECURITY TARGET DTCO 1381, Release 1.3v

Ot: Observe  
Pr: Protection marks for restricting the use of documents and products  
(D: (DIN 34: 1998-01)

		Threats															IT Objectives												
		Access	Identification	Faults	Tests	Design	Calibration_Parameters	Card_Data_Exchange	Clock	Environment	Fake_Devices	Hardware	Motion_Data	Non_Activated	Output_Data	Power_Supply		Security_Data	Software	Stored_Data	Access	Accountability	Audit	Authentication	Integrity	Output	Processing	Reliability	Secured_Data_Exchange
<SEF8> Data exchange																													
DEX_201	Secured motion data import												x																x
DEX_202	Secured motion data import												x									x							
DEX_203	Secured card data import							x																					x
DEX_204	Secured card data import							x														x							
DEX_205	Secured data export to cards							x																					x
DEX_206	Evidence of origin														x										x				
DEX_207	Evidence of origin														x										x				
DEX_208	Secured export to external media														x										x				
<SEF9> Cryptographic support																													
CSP_201	Algorithms							x			x		x					x										x	x
CSP_202	key generation							x			x		x					x										x	x
CSP_203	key distribution							x			x		x					x										x	x
CSP_204	key access							x			x		x					x										x	x
CSP_205	key destruction							x			x		x					x										x	x

This table complies to the corrigendum dated from 13.03.2004 published in the Official Journal of the EU No. L 77.

The copying, distribution and utilization of this document as well as the communication of its contents to others without expressed authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or ornamental design registration.

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
Designation Security Target DTCO 1381, Release 1.3v					
Document 40225345 SPE 000 AB			Version Pages 51 / 52		



## 11 References

- <sup>1</sup> **Appendix 10** of Annex 1B of Council Regulation (EEC) No. 3821/85 - Generic Security Targets
- <sup>2</sup> **Annex 1B** of Council Regulation (EEC) No. 3821/85 amended by CR (EC) No. 1360/2002, CR (EC) No. 432/2004 and corrigendum dated from 13.03.2004 (OJ L 77) and last amended by CR (EC) No.561/2006 and CR (EC) No. 1791/2006
- <sup>3</sup> **Council Regulation (EEC) No. 3821/85** of the 20 December 1985 on recording equipment in road transport.
- <sup>4</sup> **Council REGULATION (EC) No 2135/98** of 24 September 1998 amending Regulation (EEC) No 3821/85 on recording equipment in road transport and Directive 88/599/EEC concerning the application of Regulations (EEC) No 3820/84 and (EEC) No 3821/85
- <sup>5</sup> **Appendix 1** of Annex 1B of Council Regulation (EEC) No. 3821/85 - Data Dictionary
- <sup>6</sup> **Appendix 11** of Annex 1B of Council Regulation (EEC) No. 3821/85 - Common Security Mechanisms
- <sup>7</sup> **ITSEC** Information Technology Security Evaluation Criteria 1991

Designed by	Date	Department	Released by	Date	Department
			Winfried Rogenz	2012-04-25	I CV AM TTS LRH
	Designation				
	Security Target DTCO 1381, Release 1.3v				
Document			Version	Pages	
40225345 SPE 000 AB				52 / 52	